

The Honorable Richard A. Jones

IN THE UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

ABDIQAFAR WAGAFE, *et al.*, on behalf of
himself and other similarly situated,

Plaintiffs,

v.

DONALD TRUMP, President of the United
States, *et al.*,

Defendants.

CASE NO. C17-00094RAJ

**DECLARATION OF MATTHEW D.
EMRICH REGARDING
STIPULATED MOTION TO SEAL
PORTIONS OF THE
ADMINISTRATIVE RECORD**

I, Matthew D. Emrich, declare and say:

1. I am the Associate Director of the Fraud Detection and National Security ("FDNS") Directorate, U.S. Citizenship and Immigration Services ("USCIS"), U.S. Department of Homeland Security ("DHS"). I have held this position since November 15, 2015.

2. As the head of FDNS, I report directly to the Director of USCIS and Deputy Director of USCIS. Prior to becoming Associate Director of FDNS, beginning in November 2012, I was the Deputy Associate Director of FDNS. I first joined USCIS in May 2010, as the Chief of FDNS's Intelligence Division.

3. As the FDNS Associate Director, I am responsible for overseeing all policy, planning, management, and execution functions for FDNS. FDNS's mission is to enhance the integrity of the legal immigration system by leading USCIS' efforts to identify threats to national security and

1 public safety, detect and combat immigration benefit fraud, and remove systemic and other
2 vulnerabilities.

3 4. In *Wagafe v. Trump*, No. 2:17-cv-00094 (W.D. Wash.), I certified the administrative
4 record underlying the USCIS CARRP policy and training material in a certification dated November
5 19, 2018.

6 5. I understand the Defendants seek to file portions of the certified administrative record
7 (“CAR”) under seal pursuant to Rule 5(g) of the Local Rules of the United States District Court for
8 the Western District of Washington. The documents to be filed under seal include:

- 9 a. CAR_000010: 4/11/08 Operational Guidance for Vetting and Adjudicating Cases
10 with National Security Concerns (Guidance)
- 11 b. CAR_000075: 02/06/09 Additional Guidance on Issues Concerning the Vetting and
12 Adjudication of Cases Involving National Security Concerns
- 13 c. CAR_000104: 12/17/10 National Background Identity and Security Checks
14 Operating Procedures
- 15 d. CAR_000303: 04/01/11 Fact Sheet - Frequently Asked Questions (FAQ) CARRP
16 Policy and Operational Guidance
- 17 e. CAR_000349: 10/28/13 The Withholding of Adjudication (Abeyance) Regulation
18 Contained at 8 CFR 103.2(b)(18)
- 19 f. CAR_000366: 07/14/17 Senior Leadership Review Board Standard Operating
20 Procedures (SOP)
- 21 g. CAR_000396: 12/01/15 CARRP-Module 1 – NSD Overview
- 22 h. CAR_000414: 12/01/15 CARRP-Module 1 – NSD Overview (January 2017 update)
- 23 i. CAR_000438: 12/01/15 CARRP-Module 1 – NSD Overview (June 2017 update)
- 24 j. CAR_000463: 12/01/15 CARRP Module 2 – Handling and Protecting Sensitive
25 Information
- 26 k. CAR_000491: 12/01/15 CARRP Module 2 – Handling and Protecting Sensitive
27 Information (December 2016 and January 2017 Updates)

- l. CAR_000556: 12/01/15 CARRP Module 2 – Handling and Protecting Sensitive Information (June 2017 Update)
- m. CAR_000595: 12/01/15 CARRP Module 3 – CARRP Overview
- n. CAR_000735: 12/01/15 CARRP Module 3 – CARRP Overview (Feb 2017 update)
- o. CAR_000751: 12/01/15 CARRP Module 4 – Identifying National Security Concerns
- p. CAR_000926: 12/01/15 CARRP Module 4 – Identifying National Security Concerns (June 2016 update)
- q. CAR_001140: 12/01/15 CARRP Module 5 – Determining Eligibility and Vetting National Security Concerns
- r. CAR_001337: 12/01/15 CARRP Module 5 – Determining Eligibility and Vetting National Security Concerns (June 2017 Update)
- s. CAR_001536: 12/01/15 CARRP Module 6 – Adjudicating National Security Concerns
- t. CAR_001614: 12/01/15 CARRP Module 7 – Review and Test
- u. CAR_001674: 12/01/15 CARRP Module 7 – Review and Test (December 2016 Update)
- v. CAR_001751: 12/01/17 CARRP Module 1 – National Security and Public Safety Division Overview
- w. CAR_001767: 12/01/17 CARRP Module 2 – Handling and Protecting Sensitive Information
- x. CAR_001789: 12/01/17 CARRP Module 3 – CARRP Overview
- y. CAR_001857: 12/01/17 CARRP Module 4 – Identifying National Security Concerns
- z. CAR_001963: 12/01/17 CARRP Module 5 -- Determining Eligibility and Vetting National Security Concerns
- aa. CAR_002075: 12/01/17 CARRP Module 6 – Adjudicating National Security Concerns
- bb. CAR_002118: 12/01/17 CARRP Module 7 – Review and Test

6. Additional documents are part of the certified administrative record, but Defendants do not request to file them under seal. These documents include:

- a. CAR_000001: 4/11/08 Policy for Vetting and Adjudicating Cases with National Security Concerns
- b. CAR_000008: 04/24/08 Operational Guidance for Vetting and Adjudicating Cases with National Security Concerns (Memo)
- c. CAR_000056: 05/14/08 CARRP Operational Guidance for Vetting and Adjudicating Cases with National Security Concerns
- d. CAR_000058: 06/24/08 USCIS DOMOPS CARRP Workflows
- e. CAR_000084: 02/06/09 Attachment A - Guidance for Identifying NS Concerns
- f. CAR_000093: 2/09/09 National Security Adjudication and Reporting Requirements-Update
- g. CAR_000095: 06/05/09 Clarification and Delineation of Vetting and Adjudication Responsibilities for CARRP Cases in Domestic Field Offices
- h. CAR_000342: 07/26/11 Revision of Responsibilities for CARRP Cases Involving Known or Suspected Terrorists
- i. CAR_000345: 07/26/11 Supplemental Guidance: Revision of Responsibilities for CARRP Cases Involving Known or Suspected Terrorists

7. Many of the documents described in paragraph five, or a similar version of them, have been previously released through the Freedom of Information Act ("FOIA"), with redactions protecting information that is exempt from release. The FOIA exemptions do not overlap precisely with civil litigation privileges. I understand that more information has been provided to the Plaintiffs in the CAR than was provided through FOIA releases by USCIS.

8. Portions of the documents described in paragraph five contain information that is defined as confidential under the Stipulated Protective Order. Dkt. 86. Namely, the documents contain "sensitive, but unclassified, information to include limited official use or for official use only information" and "information compiled for law enforcement purposes, including but not limited to, investigative files and techniques related to the integrity of the legal immigration system, suspected

1 or known fraud, criminal activity, public safety, or national security, and investigative referrals.”
2 Dkt. 86, at 2(k)-(l).

3 9. Each government department or agency defines what information shall be protected and
4 how its protected information shall be handled. Within DHS, the designation “for official use only”
5 (“FOUO”) is used to identify unclassified information of a sensitive nature, not otherwise
6 categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a
7 person's privacy or welfare, the conduct of Federal programs, or other programs or operations
8 essential to the national interest.” *Safeguarding Sensitive but Unclassified (For Official Use Only)*
9 *Information*, Department of Homeland Security Management Directive System, at 1 (2005),
10 available at [https://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_110421_safeguarding_](https://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_110421_safeguarding_sensitive_but_unclassified_information.pdf)
11 [sensitive_but_unclassified_information.pdf](https://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_110421_safeguarding_sensitive_but_unclassified_information.pdf).

12 10. Information is considered FOUO when its release could cause harm and, among other
13 things, “compromise programs or operations essential to the safeguarding of our national interests.”
14 *Id.* at 4.

15 11. The documents described in paragraph five contain four categories of sensitive but
16 unclassified (“SBU”) and/or FOUO information: 1) procedures and descriptions of methods for
17 USCIS to coordinate with third party law enforcement and intelligence agencies, 2) descriptions and
18 instructions for how USCIS should interpret and rely on third party law enforcement and intelligence
19 agencies’ information, including how to handle and protect such information; 3) tools and methods
20 USCIS uses for vetting and identifying national security concerns; and 4) instructions on how to
21 operate or utilize the Fraud Detection and National Security – Database (“FDNS-DS”).

22 12. Disclosure of procedures and descriptions of methods for USCIS to coordinate with
23 third party law enforcement and intelligence agencies, and descriptions and instructions for how
24 USCIS should interpret and rely on such information, including how to handle and protect such
25 information, would reveal screening and vetting techniques that are used by the broader law
26 enforcement and intelligence community. It would further reveal how USCIS vets applications for
27 eligibility without compromising other law enforcement investigations and initiatives.

28 13. Some of this information is also derived from other law enforcement or intelligence
agencies. Revealing sensitive information owned by another agency could impair USCIS’ ability to

1 share and collect necessary information to determine if an individual is eligible for an immigration
2 benefit, and could impact other law enforcement or intelligence agencies' missions or operations.
3 Disclosure could harm the collaborative relationship between USCIS and the law enforcement
4 partners, which could degrade USCIS' ability to collect information it needs to prevent potential bad
5 actors from infiltrating the immigration system, despite not being eligible for an immigration benefit.

6 14. Disclosure of information relating to tools and methods USCIS uses for vetting and
7 identifying national security concerns would reveal internal case handling and vetting techniques for
8 evaluating whether an immigration benefit applicant may pose a threat to national security.
9 Disclosure of these techniques may allow nefarious individuals to modify their behavior and thereby
10 avoid detection.

11 15. Disclosure of information relating to instructions on how to operate or utilize FDNS-
12 DS would be harmful. FDNS-DS is USCIS' primary case management system used to record
13 requests and case determinations involving immigrant benefit fraud, public safety, and national
14 security concerns. *See Privacy Impact Assessment for the Fraud Detection and National Security*
15 *Data System (FDNS-DS)*, at 1, DHS/USCIS/PIA-013(a), May 18, 2016, *available at*
16 <https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-fdnsds-november2017.pdf>.
17 This system includes derogatory information from background checks; records from administrative
18 investigations; USCIS investigative referrals to law enforcement agencies regarding fraud, public
19 safety, and national security; referrals and leads from other government and law enforcement
20 agencies; information collected from law enforcement and intelligence agencies; referrals from the
21 public or others regarding fraud; information about fraud rates and trends; adverse information
22 identified by USCIS; and adjudicative summaries and decisions. *Id.* at 7. Access to FDNS-DS is
23 tightly constrained, even within USCIS. Public dissemination regarding how to access and navigate
24 FDNS-DS would reveal the technical capabilities of the system, the release of which could impede
25 USCIS' mission by alerting individuals to how USCIS conducts searches of its systems and any
26 limitations. In addition, if the system were hacked, it would permit the intruder to potentially
27 manipulate the way certain records are created and maintained, which could put ongoing
28 investigations at risk.

1 16. Public disclosure of the documents described in paragraph five could compromise
2 programs or operations essential to the safeguarding of our national interests. Due to the sensitive
3 nature of the information in these documents, there is a legitimate interest in protecting this
4 information from public release.

5 I declare under penalty of perjury that the foregoing is true and correct.

6 Executed this 10th day of September, 2019, at Washington, D.C.

7
8 

9 Matthew D. Emrich
10 FDNS Associate Director
11 U.S. Citizenship and Immigration Services
12 Washington, D.C.